

Linear equations in primes and dynamics of nilmanifolds

Tamar Ziegler *

Abstract. In this paper we survey some of the ideas behind the recent developments in additive number theory, combinatorics and ergodic theory leading to the proof of Hardy-Littlewood type estimates for the number of prime solutions to systems of linear equations of finite complexity.

Mathematics Subject Classification (2010). Primary 11B30, 37A30 ; Secondary 11B25, 37A45

Keywords. Multiple recurrence, arithmetic progressions, Szemerédi's Theorem, Gowers norms, Hardy-Littlewood conjectures

1. Introduction

A famous conjecture of Hardy and Littlewood [29] predicts that given a k -tuple of integers $\mathcal{H} = \{h_1, \dots, h_k\}$, there are infinitely many k -tuples

$$x + h_1, \dots, x + h_k,$$

such that all elements are simultaneously prime unless there is an obvious divisibility obstruction. Denote by $\nu_{\mathcal{H}}(p)$ the number of congruence classes modulo p that \mathcal{H} occupies, and call a k -tuple of integers admissible if $\nu_{\mathcal{H}}(p) < p$ for all primes p . Then the Hardy-Littlewood conjecture amounts to the statement that $x + h_1, \dots, x + h_k$ are simultaneously prime infinitely often if and only if \mathcal{H} is admissible. Moreover, they conjectured a precise formula for the asymptotic number of k -tuples for an admissible \mathcal{H} : Let \mathbb{P} denote the set of primes, then

$$|\{x \in [1, N], \{x + h_1, \dots, x + h_k\} \subset \mathbb{P}\}| \sim \mathfrak{S}(\mathcal{H}) \frac{N}{(\log N)^k}.$$

*The author is supported by ISF grant 407/12.

The constant $\mathfrak{S}(\mathcal{H})$ is an Euler product and is called the singular series.¹ While there have recently been extraordinary developments towards our understanding of gaps between primes and prime tuples [17, 51, 36, 37], some of them presented at the current ICM, we are still far from proving this conjecture.

One can relax the conjecture by looking for prime points in higher rank affine sublattices of \mathbb{Z}^k . In a series of papers by Green-Tao [21], [22], Green-Tao-Z [24] we prove:

Theorem 1.1 (Green-Tao-Z (2012)). *Let $\{\psi_i(\vec{x})\}_{i=1}^k$ be a collection of k affine linear forms in m variables with integer coefficients, $\psi_i(\vec{x}) = \sum_{j=1}^m a_{ij}x_j + b_i$. Suppose no two forms are affinely dependent². Then*

$$|\{\vec{x} \in [0, N]^m, \{\psi_1(\vec{x}), \dots, \psi_k(\vec{x})\} \subset \mathbb{P}\}| \sim \mathfrak{S}(\vec{\psi}) \frac{N^m}{(\log N)^k}$$

where $\mathfrak{S}(\vec{\psi})$ is an explicit Euler product (analogous to $\mathfrak{S}(H)$).

As a special case of this theorem we obtain the asymptotic number of k -term arithmetic progressions of primes. The reader will observe that the condition that no two forms are affinely dependent rules out the important case of twin primes, or more generally any k -tuple with bounded gaps as described above, however its non-homogeneous nature allows one to use it in various applications that were previously conditional on the Hardy-Littlewood conjectures (see for example [8, 30]). Theorem 1.1 may be viewed as a vast generalization of Vinogradov's 3-prime theorem [49]: any large enough odd number is a sum of three primes. We remark that very recently Vinogradov's result has been extended to include all odd numbers greater than 5 [31], thus verifying the weak Goldbach conjecture.

In this paper we give an outline of intertwining developments in ergodic theory, combinatorics and additive number theory leading to Theorem 1.1.

¹ The singular series $\mathfrak{S}(\mathcal{H})$ is given by the Euler product

$$\mathfrak{S}(\mathcal{H}) = \prod_p \left(1 - \frac{\nu_{\mathcal{H}}(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k}.$$

We refer the reader to [42] for an excellent exposition of the heuristics leading to the conjecture above. We write $a(N) \sim b(N)$ if $a(N) = b(N)(1 + o(1))$.

²Affine linear forms are affinely dependent if their linear parts are linearly dependent; e.g. the forms x and $x + 2$ are affinely dependent. A collection of k affine linear forms no two of which are affinely dependent is said to be of *finite complexity* [21].

2. Arithmetic progressions in sets of positive density

Our starting point on the combinatorial front is the following result of K. Roth [39]. Let $E \subset \mathbb{N}$. The *upper density* of E is defined to be

$$\bar{d}(E) = \limsup_{N \rightarrow \infty} \frac{|E \cap [1, N]|}{N}.$$

Theorem 2.1 (Roth 1953). *Let $E \subset \mathbb{N}$ be a set of positive upper density, then E contains a non trivial 3-term arithmetic progression.*

Roth's proof plays an important role in later developments - we outline the idea below. Let $\delta > 0$, and suppose E has density δ in an arithmetic progression P of size N , namely $E \subset P$ and $|E| = \delta N$. We first observe that if each element in P were to be chosen independently at random to be in E with probability δ then E would typically contain many 3-term progressions - approximately $\delta^3 N^2$. In view of this, Roth's argument is based on the following:

- either E has at least $\frac{\delta^3 N^2}{2}$ 3-term progressions, or
- E has density at least $\delta + c(\delta)$ on a sub-progression $Q \subset P$ of size $N^{\frac{1}{3}}$, where c is a decreasing positive function.

Our starting point is a subset $E \subset P = [1, N]$, of density δ . After running the above argument at most $s = 1/c(\delta)$ times we obtain a subset $E' \subset E$ which is of density (exactly) 1 in a subprogression $P' \subset [1, N]$ of size at least $N^{\frac{1}{3s}}$. Namely, either at some point we have many 3-term arithmetic progressions, or after finitely many steps we find an arithmetic progression of size $N^{\frac{1}{3s}}$ in E ; if N is sufficiently large then $N^{\frac{1}{3s}} \geq 3$.

We remark that a more careful analysis allows one to have the density δ depend on N in the form $\delta = 1/(\log \log N)^t$ ³.

The main issue is, of course, the second step in this argument - namely, obtaining increased density on a large subprogression. This can be achieved via discrete Fourier analysis - one considers E as a subset of $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$. Denoting 1_E the characteristic function of E , one shows that if E does not contain roughly the expected number of 3-term progressions, then the function $1_E - \delta$ has a large non trivial Fourier coefficient, namely, there exist an integer r such that

$$\left| \frac{1}{N} \sum_{x \in \mathbb{Z}_N} (1_E - \delta)(x) e^{2\pi i x \frac{r}{N}} \right| \geq c(\delta).$$

Using equidistribution properties of the sequence $\{x \frac{r}{N}\} \bmod 1$, one finds a large subprogression Q - of size $N^{\frac{1}{3}}$ - on which $x \frac{r}{N}$ is roughly constant. This in turn can

³The state of the art in the question of 3-term progressions is the recent result of T. Sanders stating that one can have the density as small as $\delta = 1/\log N^{1-o(1)}$ [41].

be translated into an increased density of at least $\delta + c(\delta)$ on (many) translates of Q . This type of argument is referred to nowadays as a *density increment argument*.

Generalizing Roth's theorem to k -term progressions for $k > 3$ turned out to be very difficult, and was shown by Szemerédi in his famous theorem [44]:

Theorem 2.2 (Szemerédi 1975). *Let E be a set of positive upper density, then E contains a non trivial k -term arithmetic progression.*

By now there are many proofs of Szemerédi's theorem. In this paper we will focus on two of them: Furstenberg's ergodic theoretic proof, which marked the beginning of the ergodic theoretic side of our story, and Gowers's proof, which pioneered the application of tools from additive combinatorics to the study of arithmetic progressions.

3. Furstenberg's proof of Szemerédi's theorem.

Shortly after Szemerédi proved the theorem on arithmetic progressions in sets of positive upper density in the integers, Furstenberg gave an ergodic theoretic proof of Szemerédi's theorem [15]. The ideas behind this proof initiated a new field in ergodic theory, referred to as *ergodic Ramsey theory*, and are the foundation of all subsequent ergodic theoretic developments on which the story in our paper is based.

Furstenberg first observed that one can translate questions about patterns in subsets of positive density in the integers to return time questions for sets of positive measure in a measure preserving system. More precisely:

Theorem 3.1 (Furstenberg correspondence principle). *Let $\delta > 0$, and let $E \subset \mathbb{N}$ be a set with positive upper density⁴. There exists a probability measure preserving system⁵ (X, \mathcal{B}, μ, T) , and a measurable set A with $\mu(A) > 0$, such that the following holds: if for some integers n_1, \dots, n_k*

$$\mu(A \cap T^{-n_1}A \cap \dots \cap T^{-n_k}A) > 0,$$

then

$$\bar{d}(E \cap (E - n_1) \cap \dots \cap (E - n_k)) > 0.$$

In particular, there exists an integer x such that $x, x + n_1, \dots, x + n_k \in E$.

⁴Furstenberg's correspondence principle as well as his multiple recurrence theorem hold in the more general context when one considers the *upper Banach density* of the set E ,

$$d^*(E) = \limsup_{N-M \rightarrow \infty} \frac{|E \cap [M, N-1]|}{N-M}.$$

We will keep to the upper density for simplicity.

⁵A probability *measure preserving system* $\mathbf{X} = (X, \mathcal{B}, \mu, T)$ consists of a probability space (X, \mathcal{B}, μ) and an invertible measurable map $T : X \rightarrow X$ with $T_*\mu = \mu$.

It follows that if we seek a $k + 1$ term arithmetic progression in E , it suffices to show that for any probability measure preserving system (X, \mathcal{B}, μ, T) , and any A with $\mu(A) > 0$, there is a positive integer n with $\mu(A \cap T^{-n}A \cap \dots \cap T^{-kn}A) > 0$. Observe that the case $k = 1$ is the famous Poincaré recurrence theorem. Indeed, Furstenberg proves the following theorem:

Theorem 3.2 (Furstenberg multiple recurrence theorem). *Let (X, \mathcal{B}, μ, T) be a measure preserving system, and let A be with $\mu(A) > 0$. Then for any $k > 0$*

$$\liminf_{N \rightarrow \infty} \frac{1}{N} \sum_{n \leq N} \mu(A \cap T^{-n}A \cap \dots \cap T^{-kn}A) > 0. \quad (1)$$

On first impression, it might seem that in replacing the arbitrary set E of positive density with an arbitrary set A of positive measure, our situation is not much improved. However, in the ergodic theoretic context one might hope to prove and apply useful structure theorems. In the case at hand - the averages (1) are studied via morphism to more structured measure preserving systems, as we will try to demonstrate below.

We will henceforth assume that the system \mathbf{X} is *ergodic*, namely any T -invariant set is of measure either 0 or 1. Any system can be decomposed to its ergodic components, thus we lose no generality in Theorem 3.2 by making this assumption.

We first briefly discuss Furstenberg's ergodic theoretic proof of Roth's theorem on 3-term progressions. We wish to evaluate the average

$$\frac{1}{N} \sum_{n \leq N} \mu(A \cap T^{-n}A \cap T^{-2n}A) = \frac{1}{N} \sum_{n \leq N} \int 1_A(x) 1_A(T^n x) 1_A(T^{2n} x) d\mu$$

where $1_A(x)$ is the characteristic function of A . Furstenberg proves that there exists a measure preserving system $\mathbf{Z} = (Z, \mathcal{B}_Z, \mu_Z, T_Z)$ that is a *Kronecker system*⁶, and a morphism⁷ $\pi : \mathbf{X} \rightarrow \mathbf{Z}$ such that for any $f_0, f_1, f_2 \in L^\infty(X)$,

$$\frac{1}{N} \sum_{n \leq N} \int f_0(x) f_1(T^n x) f_2(T^{2n} x) d\mu$$

is asymptotically the same as

$$\frac{1}{N} \sum_{n \leq N} \int \pi_* f_0(z) \pi_* f_1(T_Z^n z) \pi_* f_2(T_Z^{2n} z) d\mu_Z.$$

That is, rather than trying to evaluate the average in an arbitrary (ergodic) system, we need to evaluate it in a very special system - a compact abelian group rotation

⁶A Kronecker system $\mathbf{Z} = (Z, \mathcal{B}_Z, \mu_Z, T_Z)$ is a system where Z is a compact Abelian group, \mathcal{B}_Z the Borel σ -algebra, μ_Z the Haar measure, and T_Z is a rotation $T_Z(x) = x + \alpha$ for some $\alpha \in Z$

⁷A morphism between measure preserving systems \mathbf{X}, \mathbf{Y} is a measure preserving map between the corresponding measure spaces that intertwines the actions of T_X, T_Y . In this case \mathbf{Y} is called a *factor* of \mathbf{X} .

system: we are left with evaluating

$$\lim \frac{1}{N} \sum_{n \leq N} \int \pi_* 1_A(z) \pi_* 1_A(z + n\alpha) \pi_* 1_A(z + 2n\alpha) d\mu_Z.$$

Via Fourier analysis the above limit is easily seen to equal

$$\int \pi_* 1_A(z) \pi_* 1_A(z + b) \pi_* 1_A(z + 2b) d\mu_Z(z) d\mu_Z(b).$$

Now the projection π_* is a positive operator, namely if $f \geq 0$ then $\pi_* f \geq 0$. It follows that $\pi_* 1_A \geq 0$, and since $\int \pi_* 1_A d\mu_Z = \int 1_A d\mu = \mu(A) > 0$, the above average is clearly positive. The system $\mathbf{Z} = \mathbf{Z}(\mathbf{X})$ is called the *Kronecker factor* of \mathbf{X} and satisfies the following universal property. If \mathbf{Y} is a Kronecker system that is a factor of \mathbf{X} and $\pi_Y : \mathbf{X} \rightarrow \mathbf{Y}$ the factor map, then π_Y factors through $\mathbf{Z}(\mathbf{X})$ as demonstrated in the diagram below:

$$\begin{array}{ccc} \mathbf{X} & & \\ \pi \downarrow & \searrow \pi_Y & \\ \mathbf{Z}(\mathbf{X}) & \dashrightarrow \exists & \mathbf{Y} \end{array}$$

The factor $\mathbf{Z}(\mathbf{X})$ is constructed via the eigenfunctions of \mathbf{X} . Let us demonstrate why a non trivial eigenfunction implies the existence of a non-trivial circle rotation factor. Let ψ be an eigenfunction of \mathbf{X} ,

$$\psi(Tx) = \lambda \psi(x).$$

The function $|\psi|$ is a T -invariant function, and by ergodicity $|\psi|$ is constant a.e. Thus we can normalize ψ to take values in the unit circle. Any normalized eigenfunction gives rise to a morphism to a circle rotation system $\psi : \mathbf{X} \rightarrow (S^1, \text{Borel}, \text{Haar}, \cdot \lambda)$:

$$\begin{array}{ccc} \mathbf{X} & \xrightarrow{T} & \mathbf{X} \\ \psi \downarrow & & \downarrow \psi \\ S^1 & \xrightarrow{\cdot \lambda} & S^1 \end{array}$$

The factor $\mathbf{Z}(\mathbf{X})$ would then be the image of the map $(\psi_i) : \mathbf{X} \rightarrow (S^1)^\mathbb{N}$ given by $x \rightarrow (\psi_i(x))$, where $\{\psi_i\}$ is the collection of normalized eigenfunctions⁸ of \mathbf{X} .

⁸We implicitly assume that the system \mathbf{X} is separable and thus has at most countably many normalized eigenfunctions.

If \mathbf{X} has no non-trivial eigenfunctions, then $\mathbf{Z}(\mathbf{X})$ is trivial (a point system), and thus $\pi_* f = \int f d\mu$. In this case \mathbf{X} is called *weakly mixing*. We then have

$$\frac{1}{N} \sum_{n=1}^N \int f(x) f(T^n x) f(T^{2n} x) d\mu \rightarrow \left(\int f d\mu \right)^3,$$

and we can thus think of the points $x, T^n x, T^{2n} x$ as asymptotically independent on average. The content of Furstenberg's argument is then that if $x, T^n x, T^{2n} x$ are *not* asymptotically independent on average, then the obstruction lies in an Abelian group rotation factor. We remark that it is clear that an Abelian group rotation factor is an obstruction as in Abelian groups $z + 2n\alpha$ is determined by $z, z + n\alpha$.

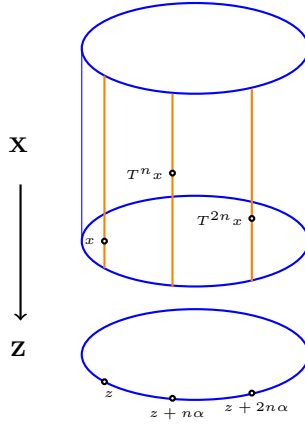


Figure 1. The points $x, T^n x, T^{2n} x$ are independent (asymptotically on average) in the fibers over the maximal Abelian group rotation factor.

To summarize, Furstenberg's proof of Roth's Theorem is based on the following dichotomy:

- either \mathbf{X} is weakly mixing, or
- there is a morphism from \mathbf{X} to a non trivial group rotation system.

The above argument motivates the following definition ([16]):

Definition 3.3 (*k*-characteristic factor). Let \mathbf{Y} be a factor of \mathbf{X} , and let $\pi : \mathbf{X} \rightarrow \mathbf{Y}$ be the factor map. We say that \mathbf{Y} is *k-characteristic* if

$$\frac{1}{N} \sum_{n=1}^N \int f_0(x) f_1(T_{\mathbf{X}}^n x) \dots f_k(T_{\mathbf{X}}^{kn} x) d\mu_{\mathbf{X}}$$

is asymptotically the same as

$$\frac{1}{N} \sum_{n=1}^N \int \pi_* f_0(y) \pi_* f_1(T_{\mathbf{Y}}^n y) \dots \pi_* f_k(T_{\mathbf{Y}}^{kn} y) d\mu_{\mathbf{Y}}.$$

We make the following observations:

- The system \mathbf{X} itself is k -characteristic for all k .
- The trivial system is 1-characteristic. In this case $\pi_* f(x) = \int f(x) d\mu_{\mathbf{X}}$, and by the *mean ergodic theorem*

$$\frac{1}{N} \sum_{n=1}^N \int f(x) f(T_{\mathbf{X}}^n x) d\mu_{\mathbf{X}} \sim \left(\int f d\mu_{\mathbf{X}} \right)^2.$$

- The Kronecker factor $\mathbf{Z}(\mathbf{X})$ is 2-characteristic (Furstenberg [15]).

The Furstenberg-Zimmer structure theorem [15, 55] relativizes the dichotomy between weak mixing and an abelian rotation factor. One can show, using spectral theory, that \mathbf{X} being weakly mixing is equivalent to the product system with the diagonal action $\mathbf{X} \times \mathbf{X}$ being ergodic. One can relativize this notion as follows. Let $\mathbf{X} \times_{\mathbf{Y}} \mathbf{X}$ be the fiber product over \mathbf{Y} . Say that $\pi : \mathbf{X} \rightarrow \mathbf{Y}$ is a *relatively weak mixing extension* if the map $\pi \times_{\mathbf{Y}} \pi : \mathbf{X} \times_{\mathbf{Y}} \mathbf{X} \rightarrow \mathbf{Y}$ is relatively ergodic, namely any $T \times T$ invariant subset in $\mathbf{X} \times_{\mathbf{Y}} \mathbf{X}$ is lifted from \mathbf{Y} via the map $\pi \times_{\mathbf{Y}} \pi$. The role of the compact abelian group rotation is replaced by the notion of an isometric extension. Say that $\pi : \mathbf{X} \rightarrow \mathbf{Y}$ is an *isometric extension* if $\mathbf{X} = \mathbf{Y} \times_{\sigma} \mathbf{M}$ where $\mathbf{M} = (M, \mathcal{B}_{\mathbf{M}}, \mu_{\mathbf{M}})$ with M a compact metric space, $\mathcal{B}_{\mathbf{M}}$ the Borel σ -algebra and $\mu_{\mathbf{M}}$ the probability measure invariant under the action of the isometry group of M , $T_{\mathbf{X}}(y, m) = (T_{\mathbf{Y}} y, \sigma(y)m)$, where σ is a (measurable) map from Y to the isometry group of M , and $\mu_{\mathbf{X}} = \mu_{\mathbf{Y}} \times \mu_{\mathbf{M}}$.

Theorem 3.4 (Furstenberg-Zimmer structure theorem [15, 55]). *There exists a sequence of factors*

$$\mathbf{X} \rightarrow \dots \rightarrow \mathbf{Z}_k(\mathbf{X}) \rightarrow \mathbf{Z}_{k-1}(\mathbf{X}) \rightarrow \dots \rightarrow \mathbf{Z}_1(\mathbf{X}) \rightarrow \star$$

such that for each k , either $\mathbf{X} \rightarrow \mathbf{Z}_k(\mathbf{X})$ is relatively weakly mixing, or there is a morphism from \mathbf{X} to a non trivial isometric extension of $\mathbf{Z}_k(\mathbf{X})$.

Theorem 3.5 (Furstenberg [15]). *The factors $\mathbf{Z}_k(\mathbf{X})$ are $(k+1)$ -characteristic.*

Observe that the factor $\mathbf{Z}_0(\mathbf{X})$ is the trivial factor and the factor $\mathbf{Z}_1(\mathbf{X})$ is the Kronecker factor. With the above structure theorem at hand it then suffices to prove the multiple recurrence theorem for systems which are towers of isometric extensions. Furstenberg utilizes this structure to show multiple recurrence - the idea being that if the multiple recurrence property holds for any k for a system \mathbf{Y} , and \mathbf{X} is an isometric extension of \mathbf{Y} , then multiple recurrence holds for \mathbf{X} as well.

4. Obstructions to 4-term progressions.

The Kronecker factor $\mathbf{Z}_1(\mathbf{X}) = \mathbf{Z}(\mathbf{X})$ is also a *universal 2-characteristic factor* : it satisfies the property that if \mathbf{Y} is any 2-characteristic factor and $\pi_{\mathbf{Y}} : \mathbf{X} \rightarrow$

\mathbf{Y} the factor map, then the factor map $\pi_Z : \mathbf{X} \rightarrow \mathbf{Z}(\mathbf{X})$ factors through \mathbf{Y} as demonstrated in the diagram below:

$$\begin{array}{ccc} \mathbf{X} & & \\ \pi_Y \downarrow & \searrow \pi_Z & \\ \mathbf{Y} & \dashrightarrow \exists & \mathbf{Z}(\mathbf{X}) \end{array}$$

The factors $\mathbf{Z}_k(\mathbf{X})$ that were constructed by Furstenberg are *not* universal $(k+1)$ -characteristic for $k > 1$. This raises the following natural problem: classify the universal $(k+1)$ -characteristic factors $Z_k(X)$. In other words, we try to understand the exact obstructions on the points $x, T^n x, \dots, T^{(k+1)n} x$ preventing them from moving about freely in X .

For the case $k = 1$, the upshot of the discussion regarding Furstenberg's proof of Roth's theorem on 3-term progressions in the previous section was that the only obstructions to the independence (asymptotically on average) of $x, T^n x, T^{2n} x$ come from a compact abelian group rotation factor, associated to the non trivial eigenfunctions of \mathbf{X} . Already in the case $k = 2$ (corresponding to 4-term progressions) we have new obstructions. Consider for example the system

$$\mathbf{Y} = (\mathbb{T} \times \mathbb{T}, \text{Borel}, \text{Haar}, T_{\mathbf{Y}})$$

where

$$T_{\mathbf{Y}} y = T_{\mathbf{Y}}(z, w) = (z + \alpha, w + 2z + \alpha),$$

where α is irrational. Iterating S we obtain

$$T_{\mathbf{Y}}^n y = T_{\mathbf{Y}}^n(z, w) = (z + n\alpha, w + 2nz + n^2\alpha).$$

We now observe that

$$y = 3T_{\mathbf{Y}}^n y - 3T_{\mathbf{Y}}^{2n} y + T_{\mathbf{Y}}^{3n} y$$

Namely, the point y is determined by the three points $T_{\mathbf{Y}}^n y, T_{\mathbf{Y}}^{2n} y, T_{\mathbf{Y}}^{3n} y$.

If there is a morphism $\mathbf{X} \rightarrow \mathbf{Y}$, these new obstructions to the (asymptotic on average) independence of the points $x, T_{\mathbf{X}}^n x, T_{\mathbf{X}}^{2n} x, T_{\mathbf{X}}^{3n} x$ will surface. Another way to see the obstructions coming from the system \mathbf{Y} is by observing that the system \mathbf{Y} exhibits *second order eigenfunctions*, namely functions ϕ satisfying $\phi(T_{\mathbf{Y}} y) = \psi(y)\phi(y)$ where ψ is an ordinary (first order) eigenfunction; for example the function $\phi(y) = \phi(z, w) = e^{2\pi i w}$ is a second order eigenfunction. Any second order eigenfunction satisfies

$$\phi(y) = \phi^3(T_{\mathbf{Y}}^n y) \phi^{-3}(T_{\mathbf{Y}}^{2n} y) \phi(T_{\mathbf{Y}}^{3n} y)$$

Thus choosing $f_0 = \phi^{-1}$, $f_1 = \phi^3$, $f_2 = \phi^{-3}$, and $f_3 = \phi$ we see that

$$\begin{aligned} 1 &= \int f_0(x) f_1(T_{\mathbf{Y}}^n y) f_2(T_{\mathbf{Y}}^{2n} y) f_3(T_{\mathbf{Y}}^{3n} x) dm \\ &= \frac{1}{N} \sum_{n \leq N} \int f_0(x) f_1(T_{\mathbf{Y}}^n y) f_2(T_{\mathbf{Y}}^{2n} y) f_3(T_{\mathbf{Y}}^{3n} x) dm. \end{aligned}$$

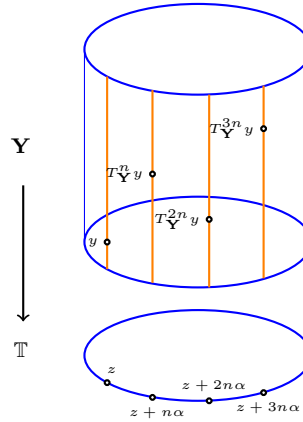


Figure 2. The points $y, T_Y^n y, T_Y^{2n} y, T_Y^{3n} y$ are not independent in the fibers over \mathbb{T} .

On the other hand one can verify that a (non trivial) 2nd order eigenfunction ϕ (and its powers) is orthogonal to ordinary eigenfunctions, thus for any $i = 0, 1, 2, 3$ the projection of the function f_i on the Kronecker factor is 0.

It turns out, however, that second order eigenfunctions are not the only obstructions. Consider the Heisenberg nilsystem: the phase space Y is the Heisenberg nilmanifold

$$Y = N/\Gamma = \begin{pmatrix} 1 & \mathbb{R} & \mathbb{R} \\ 0 & 1 & \mathbb{R} \\ 0 & 0 & 1 \end{pmatrix} \bigg/ \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$$

equipped with the Borel σ -algebra and the Haar measure, and the transformation T_Y given by $T_Y g\Gamma = ag\Gamma$, where

$$a = \begin{pmatrix} 1 & \alpha & 0 \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}.$$

Topologically Y is a circle bundle over a two dimensional torus. This system shares with the system in the above example the property that the point $g\Gamma$ is determined by $a^n g\Gamma, a^{2n} g\Gamma, a^{3n} g\Gamma$. However this dependence can not be described by a simple equation as in the previous example. Moreover, Y has *no* non-trivial second order eigenfunctions⁹.

The Heisenberg nilsystem is a special case of the following system:

$$Y = (N/\Gamma, \text{Borel}, \text{Haar}, T_Y),$$

where N/Γ a 2-step nilmanifold, and

$$T_Y : g\Gamma \rightarrow ag\Gamma \quad a \in N.$$

⁹The easiest way to see this is via equidistribution properties of polynomial orbits on nilmanifolds [34].

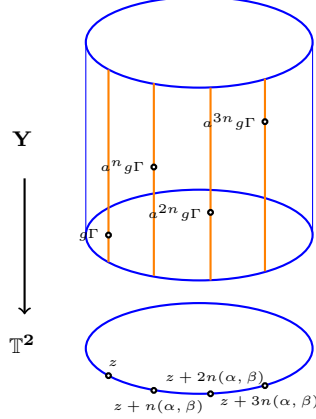


Figure 3. The points $g\Gamma, a^n g\Gamma, a^{2n} g\Gamma, a^{3n} g\Gamma$ are not independent in the fibers over the two dimensional torus.

The system \mathbf{Y} is called a 2-step nilsystem. It turns out that we need not look for further obstructions in the case $k = 2$ - all obstructions to 4-term progressions come from 2-step pro-nilsystems - inverse limits of 2-step nilsystems [16], [10, 11, 12]:

Theorem 4.1 (Conze-Lesigne, Furstenberg-Weiss). *Let \mathbf{X} be an ergodic measure preserving system. There exists a 2-step pro-nilsystem \mathbf{Y} and a morphism $\pi : \mathbf{X} \rightarrow \mathbf{Y}$ such that \mathbf{Y} is the universal 3-characteristic factor of \mathbf{X} , namely*

$$\frac{1}{N} \sum_{n=1}^N \int f(x) f(T_{\mathbf{X}}^n x) f(T_{\mathbf{X}}^{2n} x) f(T_{\mathbf{X}}^{3n} x) d\mu_{\mathbf{X}}$$

is asymptotically the same as

$$\frac{1}{N} \sum_{n=1}^N \int \pi_* f(y) \pi_* f(T_{\mathbf{Y}}^n y) \pi_* f(T_{\mathbf{Y}}^{2n} y) \pi_* f(T_{\mathbf{Y}}^{3n} y) d\mu_{\mathbf{Y}}.$$

We can now prove Szemerédi's theorem for 4-term progressions by verifying that in a 2-step nilsystem the above limit is positive (when $f = 1_A$).

Let us say a few words about the proof. By Furstenberg's structure theorem it is sufficient to study systems \mathbf{X} of the form $\mathbf{Z} \times_{\sigma} \mathbf{M}$ where $\mathbf{Z} = \mathbf{Z}_1(\mathbf{X})$ is the Kronecker factor, $T_{\mathbf{Z}}(z) = z + \alpha$, and M is a compact metric space and $\sigma : Z \rightarrow \text{ISO}(M)$. It is then shown that one can further reduce to the case where M is a compact abelian group and $\sigma : Z \rightarrow M$ satisfies a functional equation now called the Conze-Lesigne equation: for all b , a.e z

$$\sigma(z + b) - \sigma(z) = c(b) + F_b(z + \alpha) - F_b(z). \quad (2)$$

Describing how one can solve the above equation is beyond the scope of this paper, but let us hint how this equation is related to nilpotency. Consider the group

$$G = \{(b, f) : b \in Z, f : Z \rightarrow M \text{ measurable}\}$$

with the action

$$(b, f) * (c, g) = (b + c, f^c \cdot g)$$

where $f^c(z) = f(z + c)$. Then condition (2) can be interpreted as the fact that $[(\alpha, \sigma), (b, F_b)]$ is in the center of G , which hints at 2-step nilpotent behavior.

We mention another observation regarding equation (2). Upon examination one sees that

$$c(b_1 + b_2) - c(b_1) - c(b_2)$$

is an eigenvalue of $T_{\mathbf{Z}}$, and using the fact that there are only countably many of those, one can modify $c(b), F_b(z)$ so that $c(b)$ is linear in b in a neighborhood of zero in Z . A similar feature will surface in the combinatorial analysis described in section 8 below, devoted to the Inverse Theorem for the Gowers norms, which is why we mention it here.

5. Gowers proof of Szemerédi's Theorem

The next advancement (chronologically) was in the combinatorial front. Gowers gave a new proof for Szemerédi's theorem [27]. His proof is a generalization of Roth's argument to arbitrarily long arithmetic progressions using an ingenious combination of discrete Fourier analysis and additive combinatorics; in particular Gowers obtains a Roth type bound for the density of the form $1/(\log \log N)^{c(k)}$ for some constant depending on k - the length of the progression.

We first fix some notation. We denote by $[N]$ the interval $[1, N]$. For a finite set E we denote by $\mathbb{E}_{x \in E} f(x)$ the average $\frac{1}{|E|} \sum_{x \in E} f(x)$. For two functions $f, g : [N] \rightarrow \mathbb{C}$ we write $f(x) \ll g(x)$ if $|f(x)| \leq Cg(x)$ for some constant C independent of N , and we write $f(x) \ll_A g(x)$ if $|f(x)| \leq C(A)g(x)$ for some constant $C(A)$ independent of N .

In the course of the proof Gowers defines the following norms which play a very important role in further developments.

Definition 5.1 (Gowers norms). Let $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$. For $h \in \mathbb{Z}/N\mathbb{Z}$ define the discrete derivative in direction h

$$\Delta_h f(x) = f(x + h) \overline{f(x)}$$

We define the k -th Gowers uniformity norms U_k on \mathbb{C}^N by

$$\|f\|_{U^k[N]}^{2^k} = \mathbb{E}_{x, h_1, \dots, h_k \in [N]} \Delta_{h_1} \dots \Delta_{h_k} f(x)$$

Remark 5.2. One can define the Gowers norms on any abelian group; of special interest is the group \mathbb{F}_2^n where the Gowers norms are intimately related to polynomial testing.

We make a few initial observations. For 1-bounded functions f ($\|f\|_\infty \leq 1$)

- $\|f\|_{U^k[N]} = 1$ if and only if $f(x) = e^{2\pi i q(x)}$ where q is a polynomial of degree $< k$.
- By repeated application of the Cauchy-Schwarz inequality, if f correlates with $e^{2\pi i q(x)}$ where q is a polynomial of degree $< k$ then f has large Gowers norms; namely

$$|\mathbb{E}_{x \in [N]} f(x) e^{-2\pi i q(x)}| > \delta \implies \|f\|_{U^k[N]} \gg_\delta 1.$$

- If f is a random function taking the values ± 1 with probability $1/2$ for any $x \in [N]$, then by the law of large numbers, $\|f\|_{U^k[N]} = o(1)$.

The Gowers uniformity norms play an important role in the study of arithmetic progressions. If f and g are close in the U_k norm, i.e. $\|f - g\|_{U^k[N]}$ is small, then they have approximately the same number of $k+1$ term progressions. Denote by $AP_k(f)$ the number of $(k+1)$ -term progressions in f : denote

$$AP_k(f) = \mathbb{E}_{x, d \in [N]} f(x) f(x+d) \dots f(x+kd).$$

Then

$$|AP_k(f) - AP_k(g)| \ll_k \|f - g\|_{U^k[N]}. \quad (3)$$

In fact a more general statement regarding linear forms is true:

Proposition 5.3. *Let f_1, \dots, f_k be 1-bounded functions. Let $L_1(\vec{x}), \dots, L_m(\vec{x})$ be k affine linear forms in d variables with integer coefficients: $L_i(\vec{x}) = \sum_{j=1}^d l_{ij} x_j + b_i$, no two of which are affinely dependent. Then there exists $k > 0$ such that*

$$|\mathbb{E}_{\vec{x} \in [N]^d} f_1(L_1(\vec{x})) \dots f_k(L_m(\vec{x}))| \ll \min_j \|f_j\|_{U^k[N]}.$$

The proposition is proved via repeated applications of the Cauchy-Schwarz inequality, and this is where the Gowers norms enter the picture in the proof of Theorem 1.1; it is the source of the condition that no two forms are affinely dependent.

The strategy of Gowers is similar in spirit to that of Roth. The idea is as follows. Let $E \subset [N]$ be with $|E| = \eta N$. Then

- either the number of $(k+1)$ -term progressions is more than half of that expected in random set, namely $\geq \eta^{k+1} N^2/2$, or
- $\|1_E - \eta\|_{U^k[N]} \gg_\eta 1$.

In order to proceed one needs to understand the condition $\|1_E - \eta\|_{U^k[N]} \gg_\eta 1$. For $k = 2$ we observe that

$$\|f\|_{U^2[N]}^4 = \|\hat{f}\|_4^4 \leq \|\hat{f}\|_2^2 \|\hat{f}\|_\infty^2.$$

Thus if $\|f\|_2 \leq 1$ then we find that $\|f\|_{U^2[N]} \geq \eta$ implies $\|\hat{f}\|_\infty \geq \eta^2$. This implies that f has a large Fourier coefficient, namely

$$|\mathbb{E}_{x \in [N]} f(x) e(x\alpha)| \geq \eta^2.$$

For larger k the situation is much more complicated. Gowers proves the following local inverse theorem for higher Gowers norms.

Theorem 5.4 (Local inverse theorem for Gowers norms). *Let $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$ be with $|f| \leq 1$. Then*

$$\|f\|_{U^k[N]} \geq \delta \implies |\mathbb{E}_{x \in P} f(x) e^{2\pi i q(x)}| \gg_\delta 1,$$

where P is a progression of length at least N^t , $q(x)$ is a polynomial of degree $k - 1$, and t depends¹⁰ on k, δ .

The word ‘local’ in this context refers to the fact that the correlation in the above theorem is obtained not on the full interval $[N]$ but rather on a short progression of length at least N^t with $t < 1$ (for $k > 2$). This theorem provides sufficient structure to obtain increased density on a subprogression of length at least N^s : we apply Theorem 5.4 to the function $1_E - \eta$, and use the equidistribution properties of the sequence $\{q(x)\} \bmod 1$ to find an arithmetic progression of length at least N^s ($s < t$) on which $\{q(x)\} \bmod 1$ is roughly constant.

6. Classification of universal k -characteristic factors

We return now to the question of classifying k -characteristic factors. Recall that we are interested in the averages

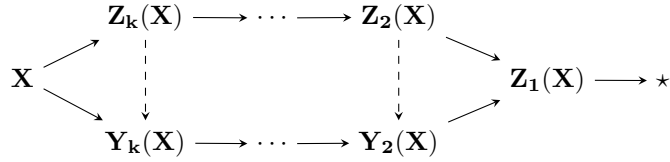
$$\frac{1}{N} \sum_{n \leq N} \int f(x) f(T^n x) f(T^{2n} x) \dots f(T^{kn} x) d\mu. \quad (4)$$

The universal 4-characteristic factors were classified by Host and Kra [33], and independently in the author’s PhD thesis [52], and were shown to be 3-step pronilsystems. Both methods were extended to work for general k - by Host and Kra in [32], and by the author in [54].

¹⁰In fact Gowers shows that one can find many such progressions: one can partition $\mathbb{Z}/N\mathbb{Z}$ into progressions P_1, \dots, P_M of average length greater than N^t , such that $\sum_{i=1}^M |\sum_{x \in P_i} f(x) e^{2\pi i q(x)}| \gg_\delta N$.

Theorem 6.1 (Host-Kra (05), Z (07)). *Let \mathbf{X} be an ergodic measure preserving system. The universal k -characteristic factor $\mathbf{Y}_k(\mathbf{X})$ is a $(k-1)$ -step pro-nilsystem.*

We have the following diagram displaying the relation between the factors $\mathbf{Z}_k(\mathbf{X})$ defined by Furstenberg in his proof of Szemerédi's theorem and the pro-nilfactors $\mathbf{Y}_k(\mathbf{X})$ which are the universal characteristic factors:



As a corollary of this structure theorem one can calculate the asymptotic formula for the averages in (4) via a limit formula for the corresponding averages on nilsystems [53].

Theorem 6.2 (Z (05)). *Let \mathbf{X} be a $(k-1)$ -step nilsystem. Then*

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n \leq N} \int f_0(x) f_1(T^n x) \cdots f_k(T^{kn} x) d\mu = \int f_0(x_0) f_1(x_1) \cdots f_k(x_k) dm_H$$

where m_H is the Haar measure on the subnilmanifold $H\Gamma^{k+1}/\Gamma^{k+1} \subset X^{k+1} = (G/\Gamma)^{k+1}$, where H is the subgroup

$$\{(g_0, g_0 g_1, g_0 g_1^2 g_2, g_0 g_1^3 g_2^3 g_3, \dots, g_0 g_1^k g_2^{\binom{k}{2}} \cdots g_{k-2}^{\binom{k}{k-2}}) : g_i \in G_i\}$$

where $\{1\} = G_{k-1} \subset G_{k-2} \subset \cdots \subset G_1 = G_0 = G$ is the derived series, i.e. $G_{i+1} = [G_i, G]$.

One can now prove Szemerédi's theorem by showing that the above limit is positive if $f_i = 1_A$ for $i = 0, \dots, k$. This approach to proving Szemerédi's theorem (and various generalizations) was taken in [6].

The proof in [54] generalizes the methods in [10, 11, 12]. Inductively, one is led to the problem of solving a functional equation similar in nature to equation (2), only the extension cocycles are now defined on a (pro)-nilmanifolds (rather than a compact abelian group). Such cocycles are in general much more difficult to handle, but one can still use the fact that orbits on products of nilmanifolds are well understood and have a nice algebraic nature (as one can see in Theorem 6.2 above).

The proof in [32] introduces seminorms, which are similar, at least semantically, to the Gowers uniformity norms¹¹

¹¹Such averages as the one below were studied in the case $k = 2$ already by Bergelson in [4].

Definition 6.3 (Host-Kra-Gowers semi-norms).

$$\|f\|_{U^k(\mathbf{X})}^{2^k} := \lim_{N \rightarrow \infty} \mathbb{E}_{h_1, \dots, h_k \in [N]} \int \Delta_{h_1} \dots \Delta_{h_k} f(x) d\mu(x).$$

It is then proved that characteristic factors for averages associated with the ergodic U_k semi-norms defined above are also pro-nilsystems. Or, in a different formulation:

$$\|f\|_{U^{k+1}(\mathbf{X})} > 0 \implies \pi : \mathbf{X} \rightarrow k\text{-step nilsystem}, \quad \pi_* f \neq 0.$$

This suggests a far reaching generalization of the Gowers local inverse theorem, which we will discuss in section 8 below.

7. The Green-Tao theorem from a characteristic factor point of view

In their famous paper, Green and Tao prove a Szemerédi's type theorem in the prime numbers [19]:

Theorem 7.1 (Green-Tao (05)). *Let $E \subset \mathbb{P}$ of positive relative density, then E contains long arithmetic progressions.*

We present the idea of the proof from a characteristic factor point of view. Our starting point will be the following version of Szemerédi's theorem: Let $f : [N] \rightarrow [0, 1]$ be a function with $|\mathbb{E}_{n \in [N]} f(x)| > \delta$. Then for any integer $k > 0$

$$AP_k(f) = \mathbb{E}_{x, d \in [N]} f(x) f(x+d) \dots f(x+kd) \geq c(\delta) + o(1) \quad (5)$$

where $c(\delta) > 0$, and is independent of N .

If we naively try to apply this theorem for a subset E of the prime numbers of relative density δ , we run into an obvious problem that $\mathbb{E}_{x \in [N]} 1_E(x) = o(1)$. We can try to fix this problem by putting a weight on each prime - we consider the von-Mangoldt function $\Lambda(x)$ which takes the value $\log p$ if x is a positive power of p and 0 otherwise. In this case we will have

$$\mathbb{E}_{x \in [N]} \Lambda(x) 1_E(x) = \delta + o(1),$$

for some constant $\delta > 0$ (independent of N). But now we face the problem that the function $\tilde{1}_E(x) = \Lambda(x) 1_E(x)$ does not take values in $[0, 1]$; in fact the function $\tilde{1}_E(x)$ is unbounded. Green and Tao show that for a certain class of unbounded functions (functions bounded by a k -psuedorandom function) one can find a "characteristic factor" for the average (5) generated by *bounded* functions ! We can summarize the procedure as follows:

- Introduce combinatorial notions of (approximate) *factor* and *projection* onto a factor.

- Find a convenient combinatorial " k -characteristic factor" for averages associated with the U_k norms, in this case a factor of functions bounded by a constant $C(k)$ (depending only on k).
- Let $\pi_*(\tilde{1}_E)$ be the (approximate) projection on the factor. Then $0 \leq \pi_*(\tilde{1}_E) \leq C(k)$, the average of the function $\pi_*\tilde{1}_E$ is approximately the same as that of $\tilde{1}_E$, namely approximately δ , and $\|\tilde{1}_E - \pi_*(\tilde{1}_E)\|_{U^k[N]}^{12}$ is small. A version of the Gowers-Cauchy-Schwarz inequality (for functions bounded by k -pseudoradnom functions) gives then, as in (3), that

$$|AP_k(\tilde{1}_E) - AP_k(\pi_*\tilde{1}_E)| \ll \|\tilde{1}_E - \pi_*\tilde{1}_E\|_{U^k[N]} \quad (6)$$

- Apply Szemerédi's Theorem to the $C(k)$ -bounded function $\pi_*\tilde{1}_E$, to obtain $AP_k(\pi_*\tilde{1}_E) \gg_\delta 1$, and thus $AP_k(\tilde{1}_E) \gg_\delta 1$

A different way to say this is that given $\epsilon > 0$ we can decompose

$$\tilde{1}_E = g + h \quad (7)$$

where g is a $C(k)$ -bounded function, and h is a function with $\|h\|_{U^k[N]} < \epsilon$. This type of theorem is now referred to as a *decomposition* theorem. There is a very nice modern and more abstract treatment of general decomposition theorems in [28], and [38] using the Hahn-Banach theorem. We remark that Theorem 7.1 has since been extended to include polynomial configurations [46], and multidimensional configurations [48, 14, 13].

8. The Inverse Theorem for the Gowers Norms

The argument in the Green-Tao theorem is based on Szemerédi's theorem which is valid for *any* subset of positive density in the integers. This has two major caveats. The first is that it can not lead to an asymptotic formula for the number of arithmetic progressions, only a lower bound. The second is that it can not be used to study non homogeneous linear configurations, since there are counter examples within periodic sets of positive density. How then can we hope to get an asymptotic formula as in Theorem 1.1 ?

We recall now that - in the ergodic theoretic context - to get a limit formula we needed to identify the universal characteristic factors. Motivated by theorem 6.1,

¹²We defined the Gowers norms for functions f on the group $\mathbb{Z}/N\mathbb{Z}$. We can define Gowers norms for functions $f : [N] \rightarrow \mathbb{C}$, setting $G := \mathbb{Z}/\tilde{N}\mathbb{Z}$ for some integer $\tilde{N} \geq 2^d N$, and defining a function $\tilde{f} : G \rightarrow \mathbb{C}$ by $\tilde{f}(x) = f(x)$ for $x = 1, \dots, N$ and $\tilde{f}(x) = 0$ otherwise. We then set

$$\|f\|_{U^d[N]} := \|\tilde{f}\|_{U^d(G)} / \|1_{[N]}\|_{U^d(G)},$$

where $1_{[N]}$ is the indicator function of $[N]$. It is easy to see that this definition is independent of the choice of \tilde{N} .

Green and Tao conjectured in 2006 that the combinatorial “universal characteristic factors” for the U_k norm come from *nilsequences* - sequences arising in a natural way from nilsystems.

Conjecture 8.1 (Inverse conjecture for the Gowers norms $(\text{GI}(s))$). *Let $s \geq 0$ be an integer, and let $0 < \delta \leq 1$. Then there exists a finite collection $\mathcal{M}_{s,\delta}$ of s -step nilmanifolds G/Γ , each equipped with some smooth Riemannian metric $d_{G/\Gamma}$ as well as constants $C(s,\delta), c(s,\delta) > 0$ with the following property. Whenever $N \geq 1$ and $f : [N] \rightarrow \mathbb{C}$ is a 1-bounded function such that $\|f\|_{U^{s+1}[N]} \geq \delta$, there exists a nilmanifold $G/\Gamma \in \mathcal{M}_{s,\delta}$, some $g \in G$ and a function $F : G/\Gamma \rightarrow \mathbb{C}$ bounded in magnitude by 1 and with Lipschitz constant at most $C(s,\delta)$ with respect to the metric $d_{G/\Gamma}$, such that*

$$|\mathbb{E}_{n \in [N]} f(n) \overline{F(g^n x)}| \geq c(s, \delta). \quad (8)$$

That is, the global obstruction (scale N) to Gowers uniformity come from sequences arising from nilsystems. Recall that the local theorem for the Gowers norms shows that local obstructions (at scale N^t) to Gowers U^{s+1} uniformity norms come from phase polynomials of degree s . We remark that the converse to Conjecture 8.1 is true and relatively easy to prove via repeated applications of the Cauchy-Schwarz inequality. Namely, if (8) holds then $\|f\|_{U^{s+1}[N]} \gg_\delta 1$. We also mention that if δ is sufficiently close to 1 then the conjecture is true; moreover, f is close (in L^1) to a genuine (unique) phase polynomial [1], and thus correlates with a (unique) phase polynomial¹³; uniqueness allows one to try an intelligent guess. In the realm when $\delta > 0$, we cannot expect uniqueness, and as it turns out, we also can't expect correlation with a genuine phase polynomial.

One can ask a similar question in the context of finite field geometry. Given a function $f : \mathbb{F}_p^n \rightarrow \mathbb{D}$ with large Gowers norm (fixing p and letting n approach ∞), what can be said about f ? It was conjectured that such functions would correlate with polynomial phase functions. More precisely:

Conjecture 8.2 (Inverse conjecture for the Gowers norms in finite fields). *Let p be a prime and let $f : \mathbb{F}_p^n \rightarrow \mathbb{C}$ be 1-bounded, with $\|f\|_{U^{s+1}[\mathbb{F}_p^n]} \geq \delta$. Then there exists a polynomial $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ of degree $\leq k$ such that*

$$|\mathbb{E}_{x \in \mathbb{F}_p^n} f(x) e^{2\pi i P(x)/p}| \geq c(s, \delta).$$

The case $s = 1$ of both conjectures follows from a short Fourier-analytic computation. The case $s = 2$ of Conjecture 8.1 was proved in [20]. The case $s = 2$ of Conjecture 8.2 was proved in [20] for odd p and for $p = 2$ in [40]. Surprisingly, Conjecture 8.2 turned out to be *false*; a counter example for the $U^4[\mathbb{F}_2^n]$ was constructed independently in [18, 35]. However, it turned out that with a small modification of Conjecture 8.2 is actually true [7, 45, 47]. Call $P : \mathbb{F}_p^n \rightarrow \mathbb{C}$ a non-standard polynomial of degree $< k$ if for all $h_1, \dots, h_s \in \mathbb{F}_p^n$ we have

$$\Delta_{h_1} \dots \Delta_{h_s} P \equiv 1$$

¹³One can exhibit a polynomial phase function $e^{p(x)}$ as a nilsequence see e.g. [24]

If $\text{char } \mathbb{F} \geq s$, then a non-standard polynomial is a standard phase polynomial, i.e. $e^{2\pi i P(x)/p}$ where $P : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ a polynomial of degree $< s$, but otherwise the class of non-standard polynomials is larger.

Theorem 8.3 (Bergelson-Tao-Z (10), Tao-Z (10,12)). *Let p be a prime and let $f : \mathbb{F}_p^n \rightarrow \mathbb{C}$ be 1-bounded, with $\|f\|_{U^{s+1}[\mathbb{F}_p^n]} \geq \delta$. Then there exists a non-standard polynomial P of degree $\leq s$, and a constant $c(s, \delta) > 0$ such that*

$$|\mathbb{E}_{x \in \mathbb{F}_p^n} f(x) e^{P(x)}| \gg c(s, \delta).$$

The proof of theorem 8.3 is via an ergodic theoretic structure theorem, similar in nature to Theorem 6.1, and a correspondence theorem - translating the finitary question to a question about limiting behavior of multiple averages for an $\oplus \mathbb{F}_p$ ergodic action.

Finally Conjecture 8.1 was proved [24]:

Theorem 8.4 (Green-Tao-Z (12)). *The inverse conjecture for the Gowers norms $GI(s)$ norms is true.*

The proof of Theorem 8.4 is long and complicated and is carried out in [24]. For a more gentle introduction to the proof we refer the reader to either [26], where the case $k = 3$ (the U^4 norm) is handled, or to the announcement in [25]. We now try to give the flavor of the proof. Suppose $\|f\|_{U^{s+1}[N]} \geq \delta$, then by definition

$$\mathbb{E}_{h \in N} \|\Delta_h f(n)\|_{U^s[N]}^{2^s} \gg_\delta 1.$$

It follows that for all h in a set H of size $\gg_\delta N$ we have $\|\Delta_h f(n)\|_{U^s[N]} \gg_\delta 1$. Now, inductively we know that, for $h \in H$, $\Delta_h f(n)$ correlates with an $s - 1$ -step nilsequence $F_h(g_h^n x_h \Gamma)$ (of complexity $\ll_\delta 1$), namely

$$|\mathbb{E}_{h \in N} \Delta_h f(n) F_h(g_h^n x_h \Gamma)| \gg_\delta 1$$

In the case $GI(2)$, this 1-step nilsequence can be taken to be $e^{2\pi i \lambda_h n}$, but in general we can't hope for anything as simple. The key difficulty now is to try to find some extra structure relating the nilsequences $F_h(g_h^n x_h \Gamma)$ for different values of h . This is already quite difficult in the $GI(2)$ case. In this case, an ingenious argument of Gowers involving tools from additive combinatorics, coupled with some geometry of numbers allows one to linearize λ_h on a nice set - a generalized arithmetic progression (GAP). This argument is then combined with a symmetry argument to construct a 2-step nilsequence $g(h)$ with $\Delta_h g(n) = e^{2\pi i \lambda_h n}$ for many values of h [20]). For general s , we follow the same strategy, however it turns out to be rather difficult to extract some algebraic structure relating the various nilsequences $F_h(g_h^n x_h \Gamma)$. An alternate approach to the inverse theorem was subsequently developed by Szegedy [9, 43]. We remark that both Theorems 8.3, 8.4 are qualitative; it is a major open question to find quantitative proofs for them.

How can one apply Theorem 8.4 to obtain Theorem 1.1? We give a very rough sketch. One needs to calculate the projection of the function $\tilde{1}_{\mathbb{P}}(n) = (\log n) 1_{\mathbb{P}}(n)$

onto the combinatorial nil-factor. It turns out that the projection essentially lies in the much smaller factor of periodic functions (with bounded period). More precisely, one first performs pre-sieving to eliminate the periodic contributions. Let $W = \prod_{p \leq w} p$ for w a slowly increasing function of N . For $(b, W) = 1$ consider $\tilde{1}_{W,b,\mathbb{P}}(n) = \tilde{1}_{\mathbb{P}}(Wn + b)$. The projection of this function on the combinatorial nil-factor should be constant, and since its average is 1 - this constant should be 1; namely one must show that

$$\|\tilde{1}_{W,b,\mathbb{P}}(n) - 1\|_{U^k[N]} = o(1).$$

Suppose $\|\tilde{1}_{W,b,\mathbb{P}}(n) - 1\|_{U^k[N]} > \delta$. Fix $\varepsilon > 0$, and decompose as in (7)

$$\tilde{1}_{W,b,\mathbb{P}}(x) - 1 = f + g$$

where f is bounded $f \ll_k 1$, and $\|g\|_{U^k[N]} < \varepsilon$. Then since U_k is a norm we get that $\|f\|_{U^k[N]} > \delta/2$. By Theorem 8.4 there is a nilsequence $F(g^n x \Gamma)$ of complexity $\ll_\delta 1$ (i.e. all parameters associated with the nilsequence such as the dimension of the nilmanifold are bounded in terms of δ), such that $|\mathbb{E}f(x)F(g^n x \Gamma)| \gg_\delta 1$. From the easy direction of Theorem 8.4 (which is valid for non bounded functions as well, via repeated applications of the Cauchy-Schwarz inequality) we have $|\mathbb{E}g(x)F(g^n x \Gamma)| < c(\varepsilon)$ (with c a decreasing function). In [22] it is shown that for any bounded complexity nilsequence we have $\mathbb{E}(\tilde{1}_{W,b,\mathbb{P}}(n) - 1)F(g^n x \Gamma) = o(1)$. Choosing ε sufficiently small in the decomposition (7), we get a contradiction.

9. Acknowledgement

I thank H. Furstenberg for introducing me to ergodic theory and to the rich subject of multiple recurrence. I thank V. Bergelson and T. Tao for their valuable comments on an earlier version of this paper.

References

- [1] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, D. Ron, *Testing low-degree polynomials over $GF(2)$* , Approximation, randomization, and combinatorial optimization, 188-199, Lecture Notes in Comput. Sci., **2764**, Springer, Berlin, 2003.
- [2] T. Austin, *On the norm convergence of nonconventional ergodic averages*, Ergodic Theory Dynam. Systems **30** (2010), no. 2, 321-338.
- [3] V. Bergelson, B. Host, B. Kra, *Multiple recurrence and nilsequences. With an appendix by Imre Ruzsa*, Invent. Math. **160** (2005), no. 2, 261-303.
- [4] V. Bergelson, *The multifarious Poincaré recurrence theorem. Descriptive set theory and dynamical systems* (Marseille-Luminy, 1996), 31-57, London Math. Soc. Lecture Note Ser., **277**, Cambridge Univ. Press, Cambridge, 2000.
- [5] V. Bergelson, A. Leibman, *Polynomial extensions of van der Waerden's and Szemerédi's theorems*, J. Amer. Math. Soc. **9** (1996), no. 3, 725-753.

- [6] V. Bergelson, A. Leibman, E. Lesigne, *Intersective polynomials and the polynomial Szemerédi theorem*, Adv. Math. **219** (2008), no. 1, 369-388.
- [7] V. Bergelson, T. Tao, T. Ziegler, *An inverse theorem for the uniformity seminorms associated with the action of \mathbb{F}_p^∞* , Geom. Funct. Anal. **19** (2010), No. 6, 1539-1596.
- [8] T. Browning, L. Matthiesen, *Norm forms for arbitrary number fields as products of linear polynomials*, arXiv:1307.7641
- [9] O. A. Camarena, B. Szegedy *Nilspaces, nilmanifolds and their morphisms*. arXiv:1009.3825
- [10] J.P. Conze, E. Lesigne, *Théorèmes ergodique por les mesures diagonales*, Bull. Soc. Math. France **112** (1984), 143-175.
- [11] J.P. Conze, E. Lesigne, *Sur un théorème ergodique pour des mesures diagonales*, Probabilités, 1-31, Publ. Inst. Rech. Math. Rennes, 1987-1, Univ. Rennes I, Rennes, 1988.
- [12] J.P. Conze, E. Lesigne, *Sur un théorème ergodique pour des mesures diagonales*, C. R. Acad. Sci. Paris, Série I, **306** (1988), 491-493.
- [13] B. Cook, A. Magyar, T. Titichetrakun, *A Multidimensional Szemerédi Theorem in the primes*, arXiv:1306.3025
- [14] J. Fox, Y. Zhao, *A short proof of the multidimensional Szemerédi theorem in the primes*, arXiv:1307.4679
- [15] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. **31** (1977), 204-256.
- [16] H. Furstenberg, B. Weiss, *A mean ergodic theorem for $1/N \sum_{n=1}^N f(T^n x)g(T^{n^2} x)$* . Convergence in ergodic theory and probability (Columbus, OH, 1993), 193-227, Ohio State Univ. Math. Res. Inst. Publ., 5 de Gruyter, Berlin, 1996.
- [17] D. Goldston, J. Pintz, C. Yıldırım, *Primes in tuples. I*, Ann. of Math. (2) **170** (2009), no. 2, 819-862.
- [18] B. Green, T. Tao, *The distribution of polynomials over finite fields, with applications to the Gowers norms*, Contrib. Discrete Math., **4**(2):1-36, 2009.
- [19] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math. **167** (2008), 481-547.
- [20] B. Green, T. Tao, *An inverse theorem for the Gowers $U^3(G)$ norm*, Proc. Edin. Math. Soc. **51** (2008), 73-153.
- [21] B. Green, T. Tao, *Linear equations in primes*, Ann. of Math. (2) **171** (2010), no. 3, 1753-1850.
- [22] B. Green, T. Tao, *The Möbius function is strongly orthogonal to nilsequences*. Ann. of Math. (2) **175** (2012), no. 2, 541-566.
- [23] B. Green, T. Tao, *The quantitative behaviour of polynomial orbits on nilmanifolds*. Ann. of Math. (2) **175** (2012), no. 2, 465-540.
- [24] B. Green, T. Tao, T. Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$ norm*, Ann. Math. (2) **176** (2012), no. 2, 1231-1372.
- [25] B. Green, T. Tao, T. Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$ norm*. Electron. Res. Announc. Math. Sci. **18** (2011), 69-90.

- [26] B. Green, T. Tao, T. Ziegler, *An inverse theorem for the Gowers U_4 -norm*. Glasg. Math. J. **53** (2011), no. 1, 1-50.
- [27] T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Func. Anal., **11** (2001), 465-588.
- [28] T. Gowers, *Decompositions, approximate structure, transference, and the Hahn-Banach theorem*, Bull. Lond. Math. Soc. **42** (2010), no. 4, 573-606.
- [29] G.H. Hardy, J.E. Littlewood, *Some problems of Paritio Numerorum (III): On the expression of a number as a sum of primes*, Acta Math. **44** (1922), 1-70.
- [30] Y. Harpaz, A. Skorobogatov, O. Wittenberg, *The Hardy-Littlewood conjecture and rational points*, arXiv:1304.3333
- [31] H. Helfgott, *The ternary Goldbach conjecture is true*, arXiv:1312.7748
- [32] B. Host, B. Kra, *Nonconventional ergodic averages and nilmanifolds*, Ann. of Math. (2) **161** (2005), no. 1, 397-488.
- [33] B. Host, B. Kra, personal communication.
- [34] A. Leibman, *Orbits on a nilmanifold under the action of a polynomial sequence of translations*, Ergodic Theory and Dynamical Systems **27** (2007), 1239-1252.
- [35] S. Lovett, R. Meshulam, A. Samorodnitsky, *Inverse conjecture for the Gowers norm is false*, STOC 2008.
- [36] J. Maynard, *Small gaps between primes*, arXiv:1311.4600.
- [37] D.H.J. Polymath, *New equidistribution estimates of Zhang type, and bounded gaps between primes*. arxiv.org/abs/1402.0811
- [38] O. Reingold, L. Trevisan, M. Tulsiani, S. Vadhan, *Dense subsets of pseudorandom sets*, Electronic Colloquium on Computational Complexity, Proceedings of 49th IEEE FOCS, 2008.
- [39] K. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104-109.
- [40] A. Samorodnitsky, *Low-degree tests at large distances*, STOC 2007.
- [41] T. Sanders, *On Roth's theorem on progressions*. Ann. of Math. (2) **174** (2011), no. 1, 619-636.
- [42] K. Soundararajan, *Small gaps between prime numbers: the work of Goldston-Pintz-Yildirim*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 1, 1-18.
- [43] B. Szegedy, *On higher order Fourier analysis*. arXiv:1203.2260
- [44] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 299-345.
- [45] T. Tao, T. Ziegler, *The inverse conjecture for the Gowers norm over finite fields via the correspondence principle*, Analysis & PDE Vol. **3** (2010), No. 1, 1-20.
- [46] T. Tao, T. Ziegler, *The primes contain arbitrarily long polynomial progressions*, Acta Math. **201** (2008) 213-305.
- [47] T. Tao, T. Ziegler, *The inverse conjecture for the Gowers norm over finite fields in low characteristic*, Ann. Comb. **16** (2012), no. 1, 121-188.
- [48] T. Tao, T. Ziegler, *A multi-dimensional Szemerédi theorem for the primes via a correspondence principle*. Israel Journal of Math, to appear.

- [49] I. M. Vinogradov, *Elements of number theory*. Translated by S. Kravetz. Dover Publications, Inc., New York, 1954.
- [50] M. Walsh, *Norm convergence of nilpotent ergodic averages*, Ann. of Math. (2) **175** (2012), no. 3, 1667-1688.
- [51] Y. Zhang, *Bounded gaps between primes*, Annals of Math, to appear.
- [52] T. Ziegler, *Non conventional ergodic averages*. PhD Thesis, Hebrew University 2003.
- [53] T. Ziegler, *A Non Conventional Ergodic Theorem for a Nil-System*, Ergodic Theory and Dynamical Systems **25** (2005) no. 4 1357-1370.
- [54] T. Ziegler, *Universal characteristic factors and Furstenberg averages*, J. Amer. Math. Soc. **20** (2007), 53-97.
- [55] R. Zimmer, *Ergodic actions with generalized discrete spectrum*. Illinois J. Math. **20** (1976), no. 4, 555-588.

Einstein Institute of Mathematics, Edmond J. Safra Campus, Givat Ram The Hebrew University of Jerusalem, Jerusalem, 91904, Israel; Mathematics Department, Technion - Israel Institute of Technology Haifa, 32000, Israel.

E-mail: tamarz@math.huji.ac.il